

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2003年 1月20日

出 願 番 号
Application Number:

特願2003-010509

[ST.10/C]:

[JP2003-010509]

出 願 人
Applicant(s):

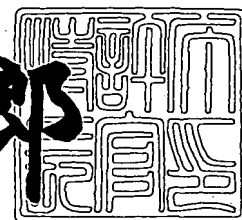
株式会社日立製作所

U.S. Appln. Filed 7-8-03
Inventor: Y. Takamoto et al
Mattingly Stanger, Major
Docket H-1105

2003年 4月25日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3030733

【書類名】 特許願

【整理番号】 H02016041A

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 高本 良史

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 山▲崎▼ 康雄

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークストレージ装置

【特許請求の範囲】

【請求項 1】

ネットワークを介して複数のクライアントにストレージを提供するネットワークストレージ装置において、

該ネットワークストレージ装置はディスク装置を有する第一の装置と複数のクライアントを接続する第二の装置から構成され、

該第一の装置は該第二の装置に上記ディスク装置の領域を割り当て、該第二の装置は該第一の装置によって割り当てられた上記領域をクライアントに割り当てるとともに、該第二の装置は上記複数のクライアントを示す複数のネットワークアドレスからのリクエストを受信し、該複数のネットワークアドレスを単一のネットワークアドレスに変換し、該第一の装置に転送することを特徴とするネットワークストレージ装置。

【請求項 2】

該第二の装置は、あらかじめ設定された該第一の装置から割り当てられた領域名を、クライアントからのアクセス要求に含まれるファイル名に追加し、該第一の装置に転送することを特徴とする請求項 1 記載のネットワークストレージ装置。

【請求項 3】

該第二の装置起動時に該第二の装置固有の装置識別子を暗号化した後に該第一の装置に転送し、該第一の装置は、該第二の装置から転送された装置識別子を復号化すると共に該第一の装置内に格納されたアクセスを許可する装置が記載されたテーブルと該第二の装置から転送された装置識別子とを比較し、該テーブルに記載された装置識別子であれば接続を許可することを特徴とする請求項 2 記載のネットワークストレージ装置。

【請求項 4】

該第一の装置は、定期的に該第二の装置に対して該装置識別子の転送を要求し、該第二の装置から応答が無い場合あるいは、該第一の装置内に格納されたアク

セスを許可する装置が記載されたテーブルと一致しない場合は、該第二の装置に割り当てた領域に対するアクセスを禁止することを特徴とする請求項 3 記載のネットワークストレージ装置。

【請求項 5】

該第一の装置は、該第二の装置起動時に該第二の装置に割り当てられた領域名を該第二の装置に転送することを特徴とする請求項 2 記載のネットワークストレージ装置。

【請求項 6】

該第一の装置は、該第二の装置起動時に該第二の装置に、該第二の装置が使用することができる容量を通知し、該第二の装置はクライアントの書き込み要求時に該使用することができる容量を超えていないかどうかを判定し、超えた場合はクライアントの書き込み要求を拒絶することを特徴とする請求項 5 記載のネットワークストレージ装置。

【請求項 7】

該第二の装置は、クライアントの書き込みあるいは読み込み要求を暗号化し、該第一の装置に転送することを特徴とする請求項 2 記載のネットワークストレージ装置。

【請求項 8】

該第二の装置は、複数の該第二の装置との間でクライアントのファイルを転送する際に、異なるネットワーク間のファイル転送かどうかを判断し、異なるネットワーク間のファイル転送の場合は、該ファイルの管理情報に記載されたユーザ識別子を変換することを特徴とする請求項 2 記載のネットワークストレージ装置。

【請求項 9】

該第二の装置は、該ファイルの転送の転送とともに、ファイルの転送元の第二の装置は転送したクライアントに関する管理情報を削除し、転送先の第二の装置はクライアントに関する管理情報を追加することを特徴とする請求項 8 記載のネットワークストレージ装置。

【請求項 10】

該第二の装置は、該第一の装置に内蔵することを特徴とする請求項2記載のネットワークストレージ装置。

【請求項11】

複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、

複数のディスク装置を管理するネットワークファイル装置と、

上記クライアントからの上記ディスク装置へのアクセス要求を中継し、該クライアントのアドレスを自己のアドレスに変換して上記ディスク装置へアクセスするクライアント管理装置を有する、ネットワークストレージ装置。

【請求項12】

複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、

複数のディスク装置を管理するネットワークファイル装置と、

上記クライアントからの上記ディスク装置へのアクセス要求を中継するクライアント管理装置を有し、

上記ネットワークファイル装置は、上記ディスク装置の所定の領域を上記クライアント管理装置に割り当て、

上記クライアント管理装置は、自己に割り当てられた上記所定の領域を分割して上記複数のクライアントに割り当てる、ネットワークストレージ装置。

【請求項13】

上記ネットワークファイル装置は、上記ディスク装置の情報の少なくとも一部のコピー情報を蓄積する1次キャッシュを有し、

上記クライアント管理装置は、上記1次キャッシュに蓄積されたコピー情報のうち、自己に割り当てられた上記所定の領域に対応する部分を蓄積する2次キャッシュを有する、請求項12記載のネットワークストレージ装置。

【請求項14】

上記ネットワークファイル装置とネットワークストレージ装置は、単一の装置として構成されているか、または、ネットワークを介して接続される分離した装置として構成されている、請求項12記載のネットワークストレージ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はネットワークストレージ装置におけるクライアントの効率的な管理方法に関する。

【0002】

【従来の技術】

【特許文献1】

特開2002-196961

【特許文献2】

特開2002-1324455

【特許文献3】

特開2001-67187

ストレージの大容量化、低価格化が進んでいる。特に磁気ディスクの分野で高い記録密度を実現する技術により、従来では実現が困難であった1筐体で数10テラバイトの装置が実現されつつある。

【0003】

一方、ネットワークの高性能化も進んでいる。比較的低価格で1ギガビット／秒～10ギガビット／秒のネットワーク転送性能の製品も出てきた。従来のネットワークでは、転送性能が10メガビット／秒～100メガビット／秒であり、大規模なデータを転送したり、多数のユーザが使用すると転送性能がネックとなり効率の良いシステムを構築することが困難であった。しかし、1ギガビット／秒～10ギガビット／秒のネットワークでは大規模データ転送や多数ユーザが使用しても十分実用に耐えうるシステムを構築できる。

【0004】

こういった背景から、ストレージとネットワークを接続し、ユーザ（クライアント）からネットワークを介して共有されたストレージ上のデータにアクセスするネットワークストレージ装置の形態が注目されている。例えば、特開2002-196961がネットワークストレージ装置の構成である。ネットワーク接続

を行う部位とサーバ処理を行う部位とデータを保存するディスク装置が単一の筐体に構成されている。クライアントは、ネットワークを介してサーバが提供する通信方法に基づいてアクセスすることで、ネットワーク上のサーバ内に格納されたデータがあたかも、自クライアント内に格納されているかのように入出力が可能となる。

【0005】

ネットワークストレージ装置の大きな課題は大規模化に向けたストレージの管理にある。ストレージが大規模化するに従って、性能の管理やクライアントの管理が複雑化する。大規模なストレージ環境に置いて、性能の管理を簡潔化する方法については、例えば特開2002-1324455に示されているように、ネットワーク上にクライアントのデータをメモリ上にキャッシングする装置を置くことで高性能化を図る方法がある。大規模化したストレージの高性能化には、基本的に本方式のように大規模なメモリによるキャッシングにより解決するケースが多い。一方、クライアントの管理については、現状では特開2001-67187に示されるように、単一の筐体は少数の管理者がクライアントの管理を行っている。

【0006】

【発明が解決しようとする課題】

小規模なストレージであれば、クライアント数も少なく少数の管理者でも管理可能である。しかし、磁気ディスクの大規模化に伴って1筐体の装置に数10テラバイトものストレージが搭載できるようになっており、こうしたケースではクライアント数は数千～数万になると予想される。ここで管理とは、クライアント毎のストレージ領域の割り当てや、割り当てられた領域に対するアクセス権限の設定などである。例えば、クライアント毎に、クライアントのネットワーク（IP）アドレス、ディスク領域名（/user/a）、アクセス権限（リード許可や書き込み許可）といった設定をクライアント毎に行う必要がある。また、クライアントの移動が発生した場合には、前記設定を移動したクライアントに対して再度設定し直す必要がある。

【0007】

【課題を解決するための手段】

上記課題を解決するために、本発明は、複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、複数のディスク装置を管理するネットワークファイル装置と、クライアントからのディスク装置へのアクセス要求を中継し、クライアントのアドレスを自己のアドレスに変換してディスク装置へアクセスするクライアント管理装置を有する。これにより、ディスク装置からは複数クライアントが1つのグループに見えるので、設定をクライアント毎に行う必要がない。

【0008】

また、本発明の他の観点は、複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、複数のディスク装置を管理するネットワークファイル装置と、クライアントからのディスク装置へのアクセス要求を中継するクライアント管理装置を有し、ネットワークファイル装置は、ディスク装置の所定の領域をクライアント管理装置に割り当て、クライアント管理装置は、自己に割り当てられた所定の領域を分割して複数のクライアントに割り当てる。これにより、ディスク装置は複数クライアントからなるグループを最小単位として取り扱い、グループに対して1つの領域を割り当てるので、設定をクライアント毎に行う必要がない。

【0009】

また、ネットワークファイル装置は、ディスク装置の情報の少なくとも一部のコピー情報を蓄積する1次キャッシュを有し、クライアント管理装置は、1次キャッシュに蓄積されたコピー情報のうち、自己に割り当てられた上記所定の領域に対応する部分を蓄積する2次キャッシュを有することとし、見かけのアクセス速度を速めることができる。ネットワークファイル装置とネットワークストレージ装置は、単一の装置として構成されていてもよいし、または、ネットワークを介して接続される分離した装置として構成してもよい。

【0010】

さらに、上記問題を解決するために、ネットワークストレージ装置はディスク装置を有する第一の装置と複数のクライアントを接続する第二の装置から構成さ

れ、第一の装置と第二の装置とでクライアントを階層管理することで多数のクライアントを効率良く管理する。第一の装置は、第二の装置への領域の割り当てやアクセス権限の設定を行い、第二の装置はクライアント毎の設定を行う。第二の装置は、通常各ネットワークエリア毎に設置され、各ネットワークエリア毎の管理だけを行う。第二の装置は、クライアントからのアクセス要求を、第一の装置に転送するが、その際第二の装置は複数のクライアントのIPアドレスを単一のIPアドレスに変換すると共に、アクセスするディスク領域名に第二の装置特有に割り当てられたディスク領域名を追加する。

【0011】

【発明の実施の形態】

【実施例1】

以下、本発明に係るクライアント管理方法の実施例1を図面に示し、さらに詳細に説明する。

【0012】

図1は、本発明によるクライアント管理方法の概略構成図を示している。101はクライアント管理装置であり、大きくはクライアント管理機構(102)、クライアント管理テーブル(103)、IPアドレス変換テーブル(120)、装置容量テーブル(104)、キャッシュ(110)から構成されている。クライアント管理装置(101)は例えばネットワーク毎に複数設置することができ、各ネットワーク毎のクライアントが使用するディスク領域や接続許可などの管理を行う。クライアント管理機構(12)は仮想ネットワークファイル機構(105)、IPアドレス変換機構(106)、管理者制御機構(107)、ネゴシエーション機構(108)、クライアント移行機構(109)から構成されている。クライアント管理装置はネットワークファイル装置(111)に接続されている。ネットワークファイル装置(111)は、クライアントのデータを保持する機能を有する。ネットワークファイル装置(111)はネゴシエーション機構(112)、ネットワークファイル機構(113)、クライアント管理テーブル(114)、キャッシュ(115)、ディスク(116)から構成されている。クライアント管理装置(101)はネットワークファイル装置(111)が提供

するディスク領域をクライアントに提供すると共に、クライアントの接続許可やクライアントの管理を行う機能を有する。

【0013】

図2は、本実施例におけるクライアント管理装置の位置づけを示している。クライアント(201～208)は各ネットワーク(209, 210)に接続されている。クライアント管理装置(211, 212)はネットワーク(209, 210)に接続され、基幹ネットワーク(213)を介してネットワークファイル装置(214)に接続される形態である。全てのクライアント(201～208)はクライアント管理装置(211, 212)を介してネットワークファイル装置(214)にアクセスされる。ネットワークは、ネットワークファイル装置(214)専用で使用される形態である。クライアント管理装置(211)は、ネットワーク(209)に接続されたクライアント(201～204)を制御・管理する。また、クライアント管理装置(212)は、ネットワーク(210)に接続されたクライアント(205～208)を制御・管理する。本実施例のクライアント管理装置により、ネットワークファイル装置の管理者は、全てのクライアント(201～208)を管理する必要はなく、クライアント管理装置(211, 212)を管理するだけで済むようになる。

一方、図3はクライアント管理装置のより一般的な使用形態である。クライアント(301～308)は各ネットワーク(309, 310)に接続されると共に、クライアント管理装置(311, 312)もクライアント(301～308)と同様に各ネットワーク(309, 310)に接続される。この形態はネットワークはネットワークファイル装置(314)専用ではなく、他の目的にも使用することができる。図2の形態に比べ、ネットワーク(309, 310, 313)がディスクアクセス以外の様々な用途に使用されるためセキュリティは図2の形態の方が高いと言える。クライアント管理装置(311)は、ネットワーク(309)に接続されたクライアント(301～304)を制御・管理する。また、クライアント管理装置(312)は、ネットワーク(310)に接続されたクライアント(305～308)を制御・管理する。本実施例のクライアント管理装置により、ネットワークファイル装置の管理者は、全てのクライアント(301

～308)を管理する必要はなく、クライアント管理装置(311, 312)を管理するだけで済むようになる。図2における形態と効果は同じである。本実施例におけるクライアント管理装置は、図2および図3の両方に対応することができる。

【0014】

図4は、一般的なネットワークファイル装置のクライアント管理テーブルの構造を示している。図1のクライアント管理テーブル(103, 114)に対応するテーブル構造である。カラム401はディスク(410)内のディスクディレクトリ(404～406)を示している。カラム402は、カラム401で示されたディレクトリを公開するクライアントのIPアドレスを示している。カラム403はディレクトリの属性を示している。read/writeは読み込みと書き込みを許すことを意味する。またreadは読み込みのみ許し、書き込みは許さないことを意味する。クライアント管理テーブルには接続された全てのクライアントを記述する必要がある。ディスク容量が増大している現在では、数万クライアントを管理することもあり、クライアント管理テーブルの管理者の負担は大きい。

【0015】

図5は、本実施例におけるクライアント管理テーブルの構造を示している。本実施例では、クライアント管理テーブルが階層化されていることが特徴である。509はネットワークファイル装置内のクライアント管理テーブル(114)を示し、501, 502はクライアント管理装置(101)内のクライアント管理テーブル(103)を示している。カラム510はネットワークファイル装置内のディレクトリを示しており、各クライアント管理装置(501, 502)へ提供するディスク領域を示している。カラム511はクライアント管理装置(501, 502)のIPアドレスを示している。カラム512はクライアント管理装置(501, 502)に対する公開属性を示している。カラム503, 506はネットワークファイル装置内のディレクトリを示しており、クライアントへ提供するディスク領域を示している。カラム504, 507はクライアントのIPアドレスを示している。カラム505, 508はクライアントに対する公開属性を

示している。本実施例では、ネットワークファイル装置（509）の管理者は、クライアント管理装置（501，502）のみ管理すれば良くなるため、管理負荷を大幅に削減できる。また、クライアントの管理者はクライアント管理装置（501，502）によって、各ネットワークの実態に即した対応が可能となる。図1におけるクライアント管理装置（101）の管理者は、管理者制御機構（107）を介してクライアント管理装置（102）の制御を行う。管理者は、通常ネットワークを介して管理者制御機構（107）にアクセスする。この際、管理者制御機構（107）は、要求者に対してユーザ識別子とパスワードの入力を要求し、認証されればクライアント管理装置（102）の制御が可能になる。他の機能としては、後述のクライアント移行機構（109）に対する指示や、処理の応答結果を受け取ることもできる。

【0016】

図6は、本実施例におけるディスクのイメージを示している。クライアントのデータは、実際は図1のディスク116内に格納されている。本実施例では、クライアント管理装置により単一のディスク（601）を、複数の仮想ディスク（602，603）を設けることができる。602および603はクライアント管理装置に対して公開された、ディスク（601）上のディレクトリである。しかし、クライアントには、602あるいは603はあたかも実際に存在するディスクのようにみせる機能をクライアント管理装置が有している。602のディレクトリを有するクライアント管理装置に管理されるクライアントの領域は604～606で示されている。また、603のディレクトリを有するクライアント管理装置に管理されるクライアントの領域は607～609で示されている。本機能は、主にセキュリティ向上を目的としている。従来のクライアント管理では、大規模ディスク内に多数のユーザデータが一元的に格納されていた。これでは、ディレクトリ属性の設定の間違いなどにより、より多数のクライアントに情報が漏れることになる。本実施例では、前述の通り単一ディスクを複数の仮想ディスクにみせることで、仮想ディスク間の参照を制限することができる。そのため、情報が漏洩する範囲を最小限に留めることができる。

【0017】

以下では図を用い、本実施例の詳細を説明する。

【0018】

図7は、仮想ネットワークファイル機構のフローを示している。ステップ701は、クライアントからのリクエストを受け付ける。ステップ702ではクライアントからのリクエストがread要求なのかwrite要求なのかを判定する。read要求であればステップ705を実行し、write要求であればステップ703を実行する。ステップ703では、書き込み要求により、該ネットワークファイル装置に割り当てられたディスク容量を算出する。これはディレクトリの容量を換算する一般的な手法により達成できる。ステップ704では、書き込み要求により、規定のディスク容量を超えていないかどうかチェックする。このチェックは、図1の装置容量テーブル104に格納された規定の容量と実際に格納しているデータ容量とこれから書き込もうとしているデータの容量からチェックする。もし、規定の容量を超えるようであればステップ707を実行し、容量が不足していることをクライアントに通知する。書き込みが可能であればステップ706を実行し、書き込み処理を行う。ステップ705は読み込み処理を行う。書き込み処理706、読み込み処理705は、後で詳細に説明する。本実施例では、ステップ704の制限を設けることによって、特定のクライアントによるディスク容量の占有を防いでいる。従来のネットワークファイル装置では、ディスクのディレクトリに対する容量制限を設けるのは困難であるが、本機能によりディスク容量を公平に分配することができるようになる。

【0019】

図8は書き込み処理のフローを示している。ステップ801はディスクアドレス変換を行う。このステップは本実施例の特徴の一つである。図6に示すように、クライアント管理装置は、ディスクを仮想化する機能を有している。クライアントがディレクトリ/user/A/file1に対して書き込みを行う場合を想定すると、クライアント管理装置は、クライアント管理装置に割り当てられたディレクトリ名である/HUB01をクライアントからのリクエストに追加し、/HUB01/user/A/file1にディスクのアドレスを変換する。この/HUB01/user/A/file1が本来のディレクトリであるが、ク

クライアントはそれを意識することはないように、ステップ801ではディスクアドレス（ディレクトリ）の変換を行っている。ステップ802では、書き込みデータをキャッシュ（110）に書き込み終了する。キャッシュに書き込まれたデータは、図9のキャッシュ書き出し処理により定期的に書き出しが行われる。

【0020】

図9は、クライアント管理装置のキャッシュ（110）に書き込まれたデータを、ネットワークファイル装置（111）に書き込む処理を行う。本処理は、例えば30秒といった定期的に実行される。ステップ901はキャッシュ（110）の空き領域判定を行う。空き領域が例えばキャッシュ（110）全体の20%以上であれば、書き込み処理を行わず終了する。空き領域が少なければ、ステップ902を実行する。ステップ902では、ネットワークパケットを生成する。クライアント管理装置とネットワークファイル装置の間はネットワークで接続されている。この間のデータ転送にはネットワークパケットを生成する必要がある。ステップ905は、データを暗号化する。これは通信のセキュリティをさらに高めるためである。ステップ903ではステップ902で生成したネットワークパケットおよびステップ905で暗号化されたパケットを送信する。ステップ904では、正常に送信できたかどうか結果を解析する。

【0021】

図10は読み込み処理のフローを示している。ステップ1001はディスクアドレス変換を示している。これは、図8のステップ801と同じ処理である。読み込みのファイルアドレスを実際にネットワークファイル装置に格納されているアドレスに変換する。ステップ1002はキャッシュに所定のデータが入っているかどうかを判定する。キャッシュに所定のデータが入っていた場合はステップ1010を実行する。キャッシュに所定のデータが入っていなかった場合はステップ1003を実行する。ステップ1003は、ネットワークパケットを生成する。これは図9のステップ902と同じである。ステップ1004はIPアドレス変換を行う。本処理は、多数のクライアントのIPアドレスを単一のIPアドレスに変換してネットワークファイル装置（111）に転送する機能である。本処理により、ネットワークファイル装置（111）は単一クライアントからの要

求のように処理できるようになる。本処理については後で詳細に説明する。ステップ1005ではネットワークパケットをネットワークファイル装置(111)に転送する。ステップ1006ではネットワークファイル装置(111)からデータを受け取り、状態を解析する。もし、エラーが発生していた場合はステップ1003からリトライする。ステップ1008では暗号化されているデータを復号化する。ステップ1009では、読み込んだデータをキャッシュに格納し、次にアクセスされた場合はキャッシュから取り出すことで読み込み処理を高速化する。ステップ1010では読み込んだデータをクライアントに転送する。

【0022】

次にIPアドレス変換機構について説明する。

【0023】

図11は、ネットワークを流れるパケットの一般的な構造を示している。1101から1104はIP(Internet Protocol)パケットを示している。また、1105から1108は、IPパケット内のデータの構造を示している。1101は、送信先のIPアドレスであり、1102は送信元のIPアドレスである。IPアドレスはネットワークに接続されたクライアントやサーバなどに付けられたネットワークの識別アドレスである。IPアドレスは、少なくとも同一ネットワーク内ではユニークでなければならない。クライアントとサーバ間、クライアント間、サーバ間などのネットワークによる通信時にはお互いのIPアドレスを指定して通信を行う。1103はIP通信時のオプションを記述する。1104はIPのデータが格納されている。通常、IPのデータ領域に直接クライアントのデータを格納することはない。IPパケットは、通信中にパケットが損失してしまっても基本的には何もしない。こういった場合、IPパケットが損失したかどうか、損失した場合の再送といった処理はIPパケットを送受信するプログラムが独自に記述する必要がある。しかし、それではネットワークにさまざまな転送方式が混在し通信の互換性が無くなったり、通信プログラムが複雑になってしまう。そこで、IPよりも高機能な処理を行うレイヤーを追加し、IPパケットをラッピングすることでネットワークの互換性や使い勝手を向上する方法が採用されている。1105から1108のデータがそのレイヤに関す

るデータであり、通常TCP (Transmission Control Protocol) データと呼ばれている。IPパケットに、再送などの機能を持ったTCPデータをラッピングすることで、使い勝手や信頼性を向上することができる。1105は、送信先のポート番号であり、1106は送信元のポート番号である。ポート番号は、ファイルサービスやメールサービスなどのサービスあるいは機能に対して割り当てられる番号と、オペレーティングシステムが独自に決める番号と2種類ある。例えば、クライアントがファイルサービスのあるサーバに対して要求する場合、送信先ポートにはファイルサービスに対応する一意の番号が割り当てられ、送信元ポートはオペレーティングシステムが使用されていないユニークな番号が割り当てられる。このポート番号は、サービスレベルで相手を特定し、お互いがTCPデータを間違いなく送受信するために使用される。1107はTCPに対応したオプションが設定される。1108はアプリケーションデータが格納される。ファイルサービスの場合は、アプリケーションデータ(1108)の領域にファイル入出力データが格納されている。

【0024】

図12は、IPアドレス変換機構のパケット送信時のフローを示している。ステップ2301は、送信パケット中から送信元のIPアドレスとポート番号を取得する。ステップ2302は、送信元のIPアドレスとポート番号をIPアドレス変換テーブルに格納する。

【0025】

図15にIPアドレス変換テーブルの構造を示す。カラム1301はクライアントのIPアドレスであり、カラム1302はクライアントのポート番号、カラム1303は変換後のIPアドレスであり、カラム1304は変換後のポート番号である。このテーブルは、変換後のパケットと要求元を判別するための対応表である。ステップ2303は、パケット中の送信元のIPアドレスをクライアント管理装置のIPアドレスに変換する。ステップ2304は、パケット中の送信元のポート番号を空きポート番号に変換する。本処理は使用中のポート番号をメモリ内に格納しておくことで実現可能である。ステップ2305は、変換後のIPアドレスとポート番号をIPアドレス変換テーブルに格納する。これらの処理

により、複数の IP アドレスを有するクライアントからの要求を単一の IP アドレスに変換することができる。

【 0 0 2 6 】

図 1 3 は、IP アドレス機構の受信時のフローを示している。ステップ 2 4 0 1 は、送信先の IP アドレスとポート番号を取得する。ステップ 2 4 0 2 は、IP アドレス変換テーブル中からステップ 2 4 0 2 で取得した IP アドレスとポート番号に一致するデータを検索する。ステップ 2 4 0 3 は、ステップ 2 4 0 2 で検索したデータのクライアント IP アドレス (1 3 0 1) とクライアントポート番号 (1 3 0 2) と、受信したパケットの送信先 IP アドレスとポート番号とを変換する。ステップ 2 4 0 4 は、IP アドレス変換テーブルの項目を削除する。これらの処理は、クライアントから発行されたパケットの IP アドレスと送信元のポート番号の組み合わせで管理することで IP アドレスを変換しても要求元を一意に特定できる特性を利用した IP アドレス変換方法である。本処理により、ネットワークファイル装置 (1 1 1) は、複数のクライアントが接続された環境でも、クライアント管理装置 (1 0 1) が IP アドレスを 1 つに変換するため、領域管理が簡単になる。

【 0 0 2 7 】

図 1 4 は、上記処理の動作を示している。クライアント (1 2 0 1) はクライアント管理装置 (1 2 2 0) に接続され、クライアント管理装置 (1 2 2 0) はネットワークファイル装置 (1 2 1 2) に接続されている。クライアント (1 2 0 1) はクライアント管理装置 (1 2 2 0) に対して読み込み要求 (1 2 0 2) を発行する。読み込み要求 (1 2 0 2) には、クライアントの IP アドレス 1 9 2 . 1 6 8 . 0 . 1 0 とクライアントのポート番号 2 0 0 0 , クライアント管理の IP アドレス 1 9 2 . 1 6 8 . 0 . 1 0 0 とサービスを示すポート番号 8 0 と、クライアント (1 2 0 1) が読み込みを要求するファイル名 / u s e r / A が格納されている。クライアント (1 2 0 1) からは、あたかもクライアント管理装置 (1 2 2 0) がディスクを有しているように見える。この要求を受けたクライアント管理装置 (1 2 2 0) は仮想ネットワークファイル機構 (1 2 0 4) により、ディスクアドレスが変換されパケット 1 2 0 6 のように読み込みアドレス

に／HUB01が追加され／HUB01／user／Aに変換される。もし、／HUB01／user／Aがキャッシュ1220に格納されていた場合は、クライアント1201にデータが返送されるが、キャッシュ1220に格納されていなかった場合はIPアドレス変換機構(1208)にパケットが渡される。ここで、IPアドレス変換が行われ、パケット1210のように、送信元アドレスはクライアント管理装置(1220)自身のIPアドレスである192.168.10.10に変換され、送信元ポート番号はクライアント管理装置(1220)内で未使用の10000が割り当てられる。また送信先IPアドレスはネットワークファイル機構(1212)のIPアドレスが設定される。この変換結果は、IPアドレス変換テーブル(1209)に格納される。送信先ポート番号は、クライアント(1201)が発行した、送信先ポート番号80と同じである。このパケット(1210)を受け取ったネットワークファイル装置(1212)は、／HUB01／user／Aのファイルを読み込み、パケット1211に読み込んだデータ(data)を格納して直接の要求元であるクライアント管理装置(1220)に返送する。クライアント管理装置(1220)は、ネットワークファイル装置(1212)からパケットを受け取るとIPアドレス変換機構(1208)とIPアドレス変換テーブル(1209)により、クライアントのIPアドレスとクライアントが発行した時のポート番号に変換されパケット1207が生成される。このパケット(1207)は仮想ネットワークファイル機構(1204)を介してクライアント(1201)に返送される。このように、クライアント管理装置(1220)によって、クライアントにはあたかもディスクがクライアント管理装置(1220)にあるかのように見せ、ネットワークファイル装置(1212)には複数のクライアントが接続されたようには見せなくすることができる。

【0028】

図16はクライアント管理装置(102)におけるネゴシエーション機構(108)のフローを示している。ネゴシエーション機構の目的は、クライアント管理装置(102)とネットワークファイル装置(111)間の通信を正しく確立することにある。ネットワーク上を流れるパケットが第3者に見られてしまった

り、クライアントを偽ってデータを読み出そうとする行為を検出し接続できなくする処理を行う。本フローは、ネットワークファイル装置（１１１）に接続を開始するとき、ネットワークファイル装置（１１１）から一定期間毎に呼び出される。ステップ１４０１は装置識別要求かどうかを判断する。装置識別要求とは、ネットワークファイル装置（１１１）から定期的に呼び出され、ネットワークファイル装置（１１１）に対して装置識別子を転送する要求である。装置識別要求であればステップ１４０７を実行し、そうでなければステップ１４０２を実行する。ステップ１４０２以降の処理は、ネットワークファイル装置（１１１）と最初に接続する時に実行される。ステップ１４０２はネットワークファイル装置（１１１）に対してコネクションの開始を要求する。ステップ１４０３は、装置識別子を暗号化する。装置識別子とは、クライアント管理装置特有の識別子で、クライアント管理装置とネットワークファイル装置の間だけで使用される。ステップ１４０４は、ステップ１４０３で暗号化された装置識別子をネットワークファイル装置に転送する。ステップ１４０５は、ネットワークファイル装置とコネクションが確立したかどうかを判定する。これは、送信した装置識別子がネットワークファイル装置に認定された場合、コネクション許可を通知することによって実現できる。コネクションが確立された場合ステップ１４０６を実行し、クライアント管理装置が使用可能な装置容量とクライアント管理装置のルートディレクトリを送信する。ルートディレクトリは、図１０のステップ１００１等で使用される。また、ネットワークファイル装置（１１１）から定期的に呼び出されるフローもある。ステップ１４０７以降は、ネットワークファイル装置（１１１）から定期的に呼び出されるフローである。このフローの目的は、ＩＰアドレスを偽ったアクセスを排除することである。ステップ１４０１以降の処理は、クライアント管理装置の起動時に実行されるが、起動後も定期的に装置識別子を送信することで常に正しい接続を保つためである。ステップ１４０７は装置識別子を暗号化する。ステップ１４０８はステップ１４０７で暗号化された装置識別子をネットワークファイル装置（１１１）に送信する。

【００２９】

図１７は、ネットワークファイル装置（１１１）におけるネゴシエーション機

構（112）のフローを示している。ステップ1501はクライアント管理装置からのコネクション要求を受け付ける。ステップ1502はクライアント管理装置から転送された装置識別子が格納されたデータを復号化する。ステップ1503は復号化された装置識別子が正しいかどうか確認し、ステップ1504で正しいクライアント管理装置からの要求であればステップ1505を実行し、正しくなかった場合はステップ1511で不正アクセスと判断し装置を閉塞する。ここで、閉塞の範囲は任意である。例えば、装置全体を閉塞し全てのアクセスを停止させることも考えられるし、該当するクライアント管理装置に割り当てた領域だけ停止することも考えられる。ステップ1505は、クライアント管理装置に対して、使用可能なディスクの容量とルートディレクトリを送信する。ステップ1509は一定期間処理を停止する。ステップ1506はクライアント管理装置に対して装置識別子を要求する。ステップ1507は装置識別子が正しいかどうかを確認する。ステップ1508で正しいクライアント管理装置からの要求であればステップ1509を実行し、そうでなければステップ1510で装置を閉塞する。こうすることで、クライアント管理装置起動後にIPアドレスを偽ったアクセスが発生しても、ネットワークファイル装置とクライアント管理装置しか知らない装置識別子を確認しあうことで不正アクセスを検知でき、データが不正に読まれたり改竄されることを防ぐことができる。

【0030】

次に、本発明におけるもう一つの特徴であるユーザ移行機構について説明する。

【0031】

図18は、ネットワーク間でユーザが移行する場合のネットワークファイルの管理を示している。1601～1603は移行元のクライアント管理テーブルであり、1604～1606は移行先のクライアント管理テーブルである。1610はディスクであり、1608は移行元のクライアント管理装置に割り当てられたディスク領域であり、1609は移行先のクライアント管理装置に割り当てられたディスク領域である。1612は、移行元のクライアントが保有するデータであり、1623はデータの移行先を示している。異なるネットワーク間でクラ

クライアントが移行する場合、まず、1607に示すようにクライアント管理テーブルの該当クライアントを移行する。その後、データの移行のため、1611に示すように移行元のディスク領域1612から該当クライアントが保有するデータを吸い上げた後、移行先であるディスク領域1613にデータをコピーする。データのコピーの際に、必要な処理としてユーザ識別子の変換がある。ユーザ識別子は、ネットワーク毎に決められたユーザ毎にユニークな番号である。ユーザ識別子はユーザが保有するファイル毎に設定されており、この情報はネットワークファイル機構がディスク内に格納している制御情報である。

【0032】

図19はファイルの管理テーブルの構造を示している。カラム1701はファイル名であり、カラム1702はユーザ識別子であり、カラム1703はファイルの属性を示している。ユーザ識別子1702はネットワーク毎にそのネットワークの管理者が定めたユーザ毎にユニークな番号であるネットワークファイル機構(113)はユーザ識別子を使用して、ファイルのアクセス権限を管理している。カラム1703はファイルの属性であり、例えば、rはリードを許可し、wは書き込みを許可するといったことを意味する。クライアント管理テーブルの更新は通常は管理者が行い、データの移行は通常はクライアント自身が行わなくてはならない。データ移行方法の一例として、まずクライアントが移行元のデータをクライアント自身にコピーする。次にクライアントはネットワークの移行を行う。この際、クライアントは移行先のネットワークの管理者から新しいユーザ識別子を教えてもらう。クライアントは、クライアント内のファイルについて、新しいユーザ識別子に変換する。この時点で、先にコピーしたファイルのユーザ識別子が新しいユーザ識別子に変換される。その後、コピーしたファイルを移行先のネットワークファイル装置(111)に転送し、全ての移行処理が完了する。このように、現状のクライアント移行処理はクライアント自身の負担が大きい。

【0033】

図20はクライアント管理装置(102)内のクライアント移行機構の移行元のフローを示している。ステップ1802は管理者から要求を受け付ける。管理者から要求とは、クライアント管理テーブル内の移行したいクライアントのリス

トなどである。ステップ1802は、移行先のクライアント管理装置に対して、ステップ1801で受け取った移行対象のクライアント情報とともに問い合わせを行う。ステップ1803は移行先のクライアント管理装置から、移行を了承するかどうかの応答を待つ。このとき、管理者はクライアントの移行が可能な場合、クライアント管理装置に対してクライアントの新しいユーザ識別子を通知する。ステップ1804は、移行が可能かどうかを判定し、移行が可能であればステップ1805を実行し、移行できない場合はステップ1809を実行する。ステップ1805は移行対象のクライアントのデータを読み込む。ステップ1806は移行先のクライアント管理装置に対して、ステップ1805で読み込んだデータを送信する。ステップ1807は移行先のクライアント管理装置から該当するクライアントのデータ移行が完了したかどうかの応答を待つ。ステップ1808は移行元のクライアント管理装置内のクライアント管理テーブルから、移行を終了したクライアントの情報を削除する。ステップ1809は、クライアント管理装置の管理者に対して、移行結果を通知する。

【0034】

図21はクライアント管理装置(102)内のクライアント移行機構の移行先のフローを示している。ステップ1901は移行元のクライアント管理装置から移行の要求を受け付ける。この要求には、移行元から移行したいクライアントの情報が含まれる。ステップ1902は、移行先のクライアント管理装置の管理者に対して、移行するかどうかを問い合わせる。ステップ1903は管理者からの応答を待つ。ステップ1904は移行可能かどうかを判断し、移行可能であればステップ1920を実行し、そうでないならステップ1909を実行する。ステップ1920は移行元のクライアント管理装置に対して、クライアントの移行が可能であることを通知する。ステップ1905は、移行元のクライアント管理装置からクライアントのデータを受信する。ステップ1906は受信したデータのユーザ識別子を、ステップ1802で通知された新しいユーザ識別子に変換する。ステップ1907はユーザ識別子変換されたクライアントのデータの書き込みを行う。ステップ1908は、移行元のクライアント管理装置に対して、クライアントのデータの移行が完了したことを通知する。ステップ1909は、クラ

クライアント管理装置内のクライアント管理テーブルに移行したクライアントの情報を追加する。ステップ 1 9 1 0 は管理者へクライアントの移行が完了したことを通知する。これらの処理により、クライアント管理装置間でクライアント管理テーブルの更新やクライアントのデータ移行が可能となり、クライアントは移行のための処理を行う必要がなくなる。本実施例では、データ移行時にユーザ識別子を変更する手順を述べたが、ネットワークを移動しない場合はユーザ識別子が変わらないためユーザ識別子を変更する必要はない。ネットワークを判定し、同一ネットワーク内での移動であればユーザ識別子の移動は行わず、異なるネットワークの場合のみユーザ識別子の変更を行うこともできる。

【 0 0 3 5 】

本実施例 1 では、ネットワークファイル装置と、ネットワークファイル装置に接続されたクライアント管理装置において、多数のクライアントを管理する方法として、クライアント管理装置とネットワークファイル装置とでクライアントの管理を階層化することで管理負荷を低減する方法を述べている。本実施例の効果として、クライアント管理装置とネットワークファイル装置間を暗号化することで、多数のネットワーククライアントが接続されたネットワークを介しても安全にファイルアクセスができ、かつクライアント管理負荷も低減できる。また、クライアント管理装置内に設けたキャッシュにより、クライアントから頻繁にアクセスされるデータはキャッシュに格納されるため、アクセス性能を高める効果がある。ネットワークファイル装置は特定のクライアント管理装置からのみデータへの読み書きを許可する形態であるため、クライアント管理装置以外のクライアントから読み書きされることはない。そのため、クライアント管理装置を介さないアクセスがないことを保証できるため、クライアント管理装置内のキャッシュに不整合が生じることはない。また、大規模なディスク領域を複数の領域に分割し、分割したそれぞれの領域を各クライアント管理装置が管理可能となる。領域には使用可能な最大容量を設定することができるため、ネットワークファイル装置の管理者は大規模なディスク領域を管理し易くなる。

〔実施例 2〕

実施例 2 では、実施例 1 におけるクライアント管理装置（1 0 2）がネットワ

ークファイル装置（111）に内蔵されたケースについて述べる。実施例2では、クライアント管理装置がネットワークファイル装置に内蔵されているため、大規模ディスクの管理負荷を抑えつつ、実装コストを低減することができる。

【0036】

図22はネットワークファイル装置（2101）の構成図を示している。ネットワークファイル装置（2101）は、クライアント管理機構（2102）、クライアント管理テーブル（2103、2110）、IPアドレス変換テーブル（2120）、装置容量テーブル（2104）、ネットワークファイル機構（2109）、キャッシュ（2111）から構成される。ネットワークファイル装置（2101）には複数のディスク（2112）が接続されている。各構成図の動作は実施例1と同様である。ただし、実施例1における暗号化処理は、実施例2では実行しなくても構わない。これは、暗号化処理はネットワークを流れるデータを保護することが大きな目的であり、実施例2のようにクライアント管理機構（2102）がネットワークファイル装置（2101）に内蔵されている場合は、通信中のデータを第3者が見ることができないためである。そのため、実施例1に比べ暗号化の処理が削減できるため処理を高速化することができる。さらに、実施例では、各クライアント管理装置毎にキャッシュが設けられていたが、実施例2ではネットワークファイル装置が有するキャッシュを使用できるため、機構を簡単化することができる。実施例2でも、クライアントの管理方法は実施例1と同じである。ネットワークファイル装置（2101）の管理者は、ネットワークファイル装置（2101）に接続されたディスク（2112）の領域をクライアント管理機構（2102）に提供するだけであり、実際のクライアント管理はクライアント管理機構の管理者が行うことで、大規模クライアントの管理を階層化できる。クライアント管理機構は複数でも構わない。ネットワーク毎にクライアント管理機構（2102）を設けることで、多数のネットワーク上のクライアントを階層管理できるようになる。それぞれの管理者は、ネットワークを介して、ネットワークファイル機構（2109）やクライアント管理機構（2102）にアクセスすることができる。

【0037】

図 2 3 は、本発明の実施例 2 におけるネットワークの構成図を示している。全てのクライアント (2 2 0 1) は、ネットワーク (2 2 0 3) を介して直接ネットワークファイル装置 (2 2 0 4) に接続している。実施例 1 に比べ、簡単なネットワーク構成で本発明の効果を得ることができる。

【 0 0 3 8 】

【発明の効果】

本発明により、大規模なネットワークストレージのクライアントを階層管理することができ、これにより効率的なクライアント管理が行えるようになる。

【図面の簡単な説明】

【図 1】

本発明の実施例 1 における全体構成図を示す。

【図 2】

本発明のネットワーク構成の例を示す。

【図 3】

本発明のネットワーク構成の例を示す。

【図 4】

ネットワークファイル装置のクライアント管理情報を示す。

【図 5】

実施例 1 におけるクライアント管理情報の構成を示す。

【図 6】

実施例 1 におけるディスク管理の構成を示す。

【図 7】

仮想ネットワークファイル機構のフローを示す。

【図 8】

書き込み処理のフローを示す。

【図 9】

キャッシュ書き出し処理のフローを示す。

【図 1 0】

読み込み処理のフローを示す。

【図 1 1】

ネットワークパケットの構成を示す。

【図 1 2】

IP アドレス変換機構の送信時のフローを示す。

【図 1 3】

IP アドレス変換機構の受信時のフローを示す。

【図 1 4】

実施例 1 における IP アドレスとファイル名の変換手順を示す。

【図 1 5】

IP アドレス変換テーブルの構成を示す。

【図 1 6】

クライアント管理装置のネゴシエーション機構のフローを示す。

【図 1 7】

ネットワークファイル装置のネゴシエーション機構のフローを示す。

【図 1 8】

クライアント移行時の手順を示す。

【図 1 9】

ファイルの管理テーブルの構造を示す。

【図 2 0】

クライアント移行機構の移行元のフローを示す。

【図 2 1】

クライアント移行機構の移行先のフローを示す。

【図 2 2】

実施例 2 の全体構成図を示す。

【図 2 3】

実施例 2 のネットワーク構成を示す。

【符号の説明】

101 はクライアント管理装置、111 はネットワークファイル装置、102 はクライアント管理機構、103 および 114 はクライアント管理テーブル、1

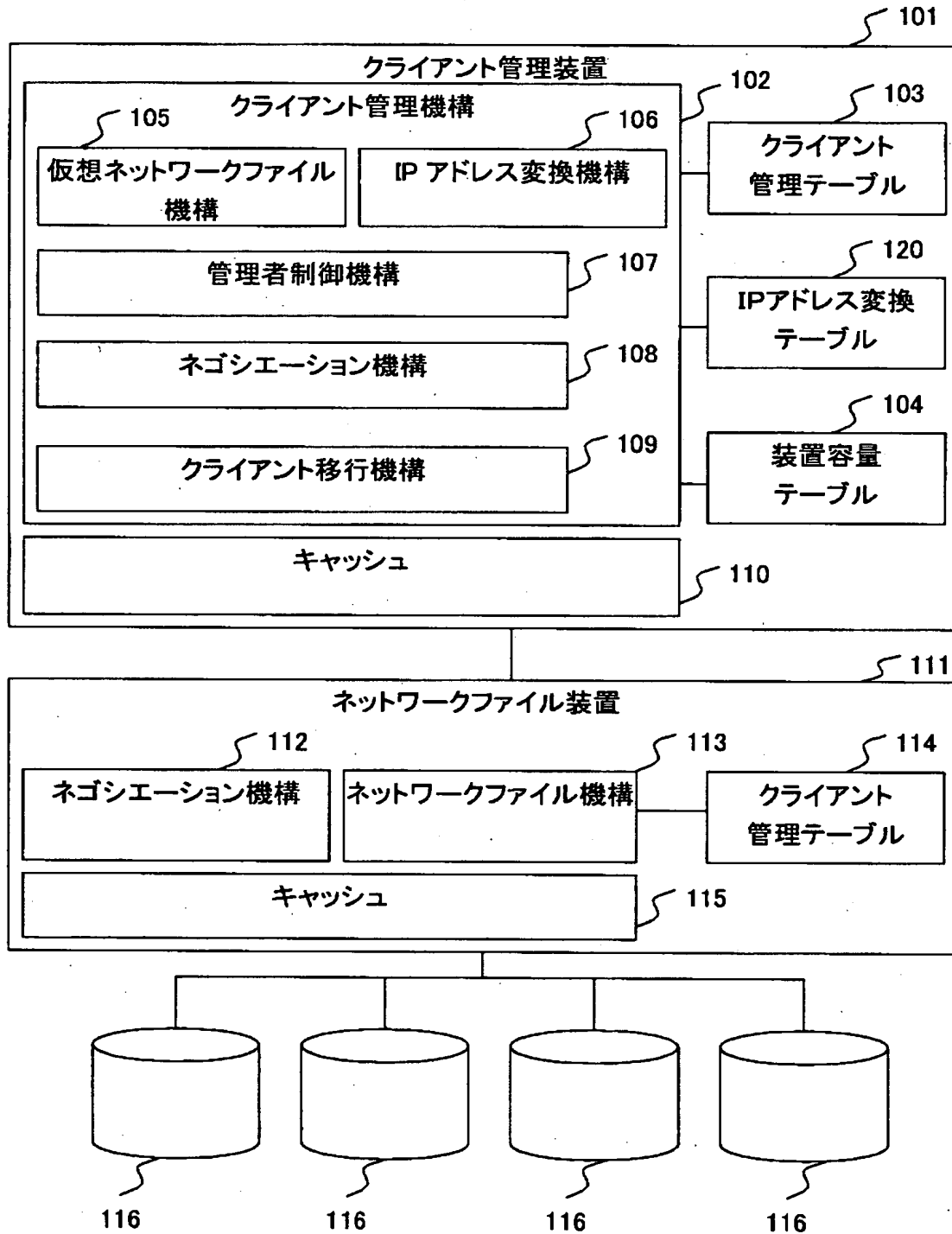
20はIPアドレス変換テーブル，104は装置容量テーブル，105は仮想ネットワークファイル機構，106はIPアドレス変換機構，107は管理者制御機構，109はクライアント移行機構，110および115はキャッシュ，108および112はネゴシエーション機構，113はネットワークファイル機構を示している。

【書類名】

図面

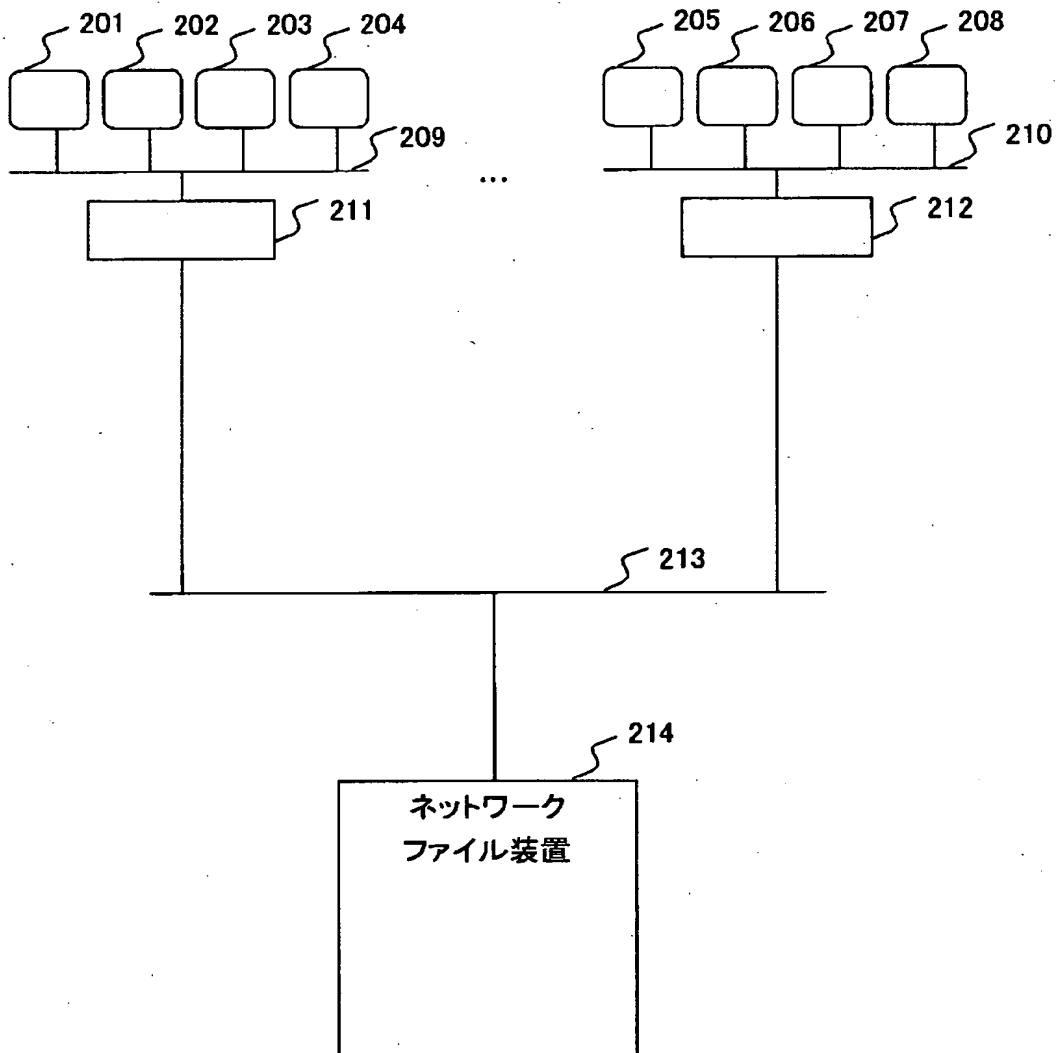
【図 1】

図 1



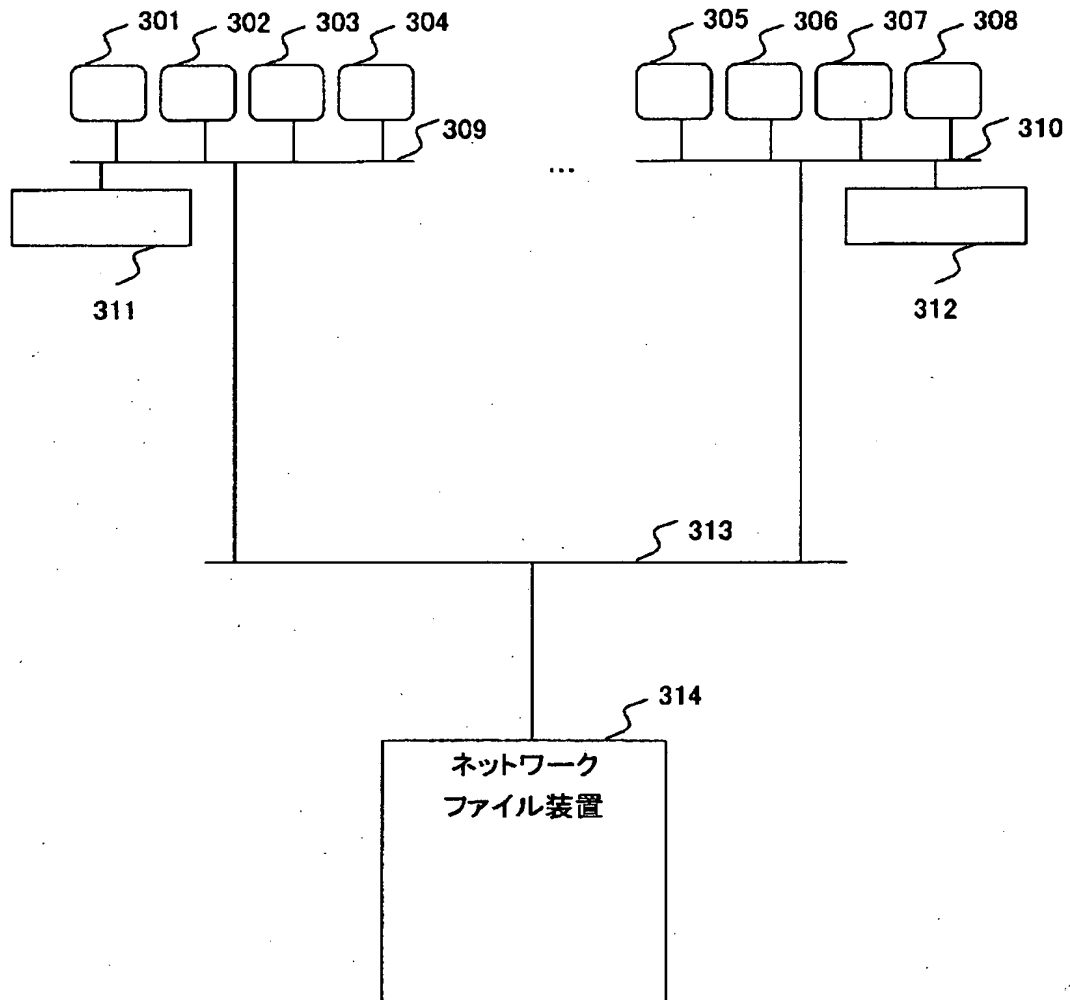
【図 2】

図 2



【図 3】

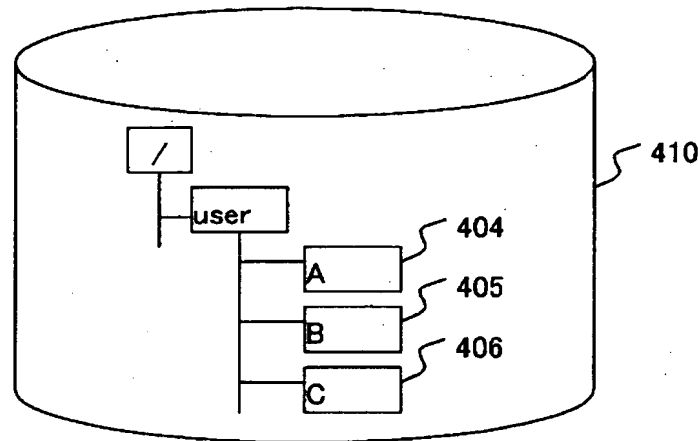
図 3



【図 4】

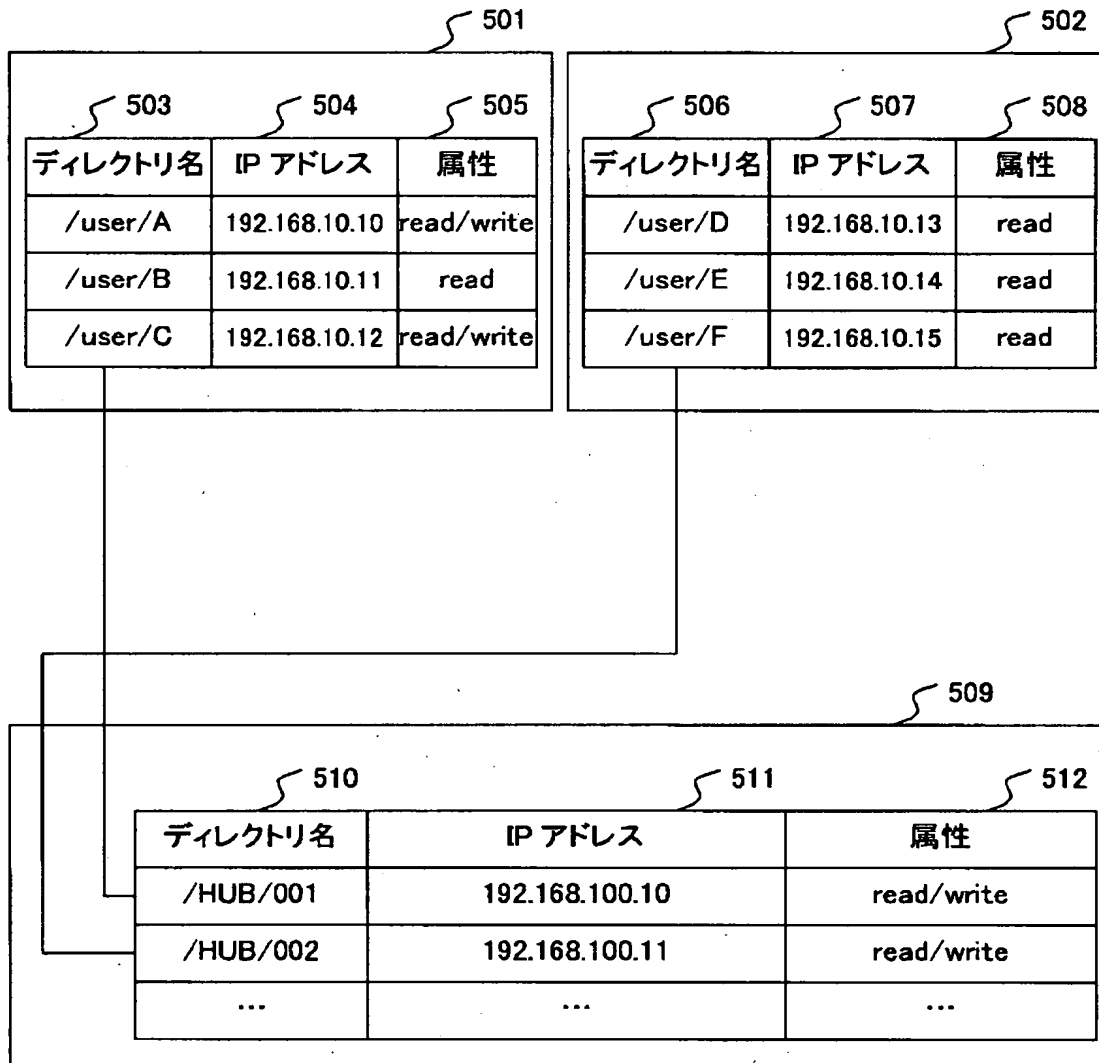
図 4

ディレクトリ名	IP アドレス	属性
/user/A	192.168.100.10	read/write
/user/B	192.168.100.11	read
/user/C	192.168.100.12	read/write
...



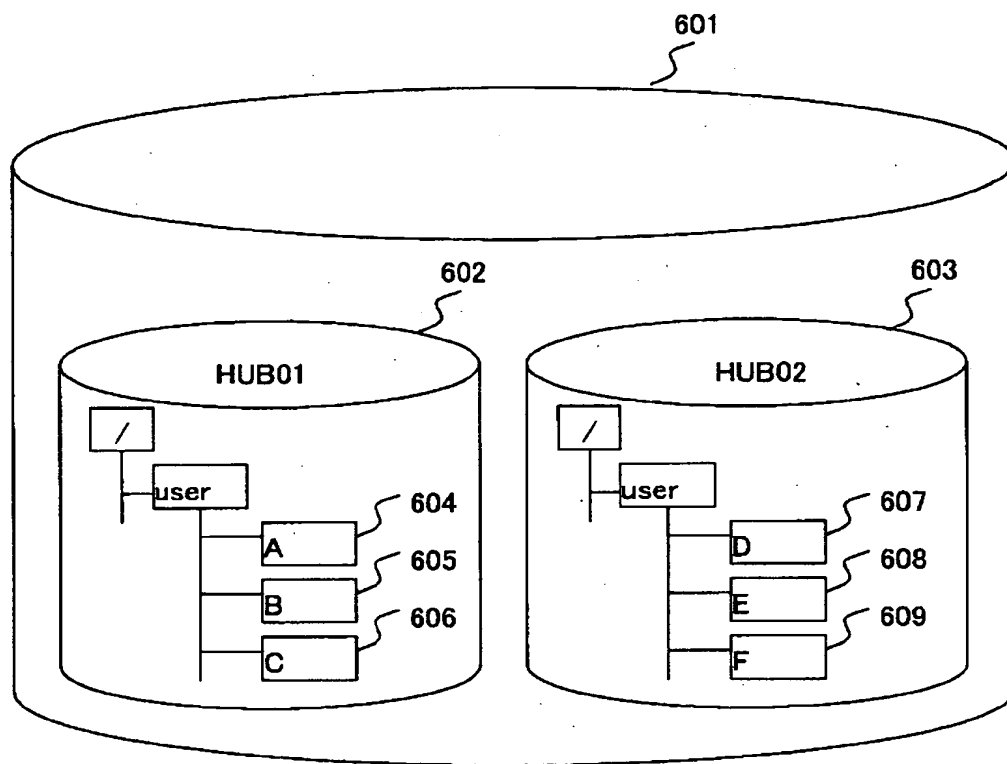
【図 5】

図 5

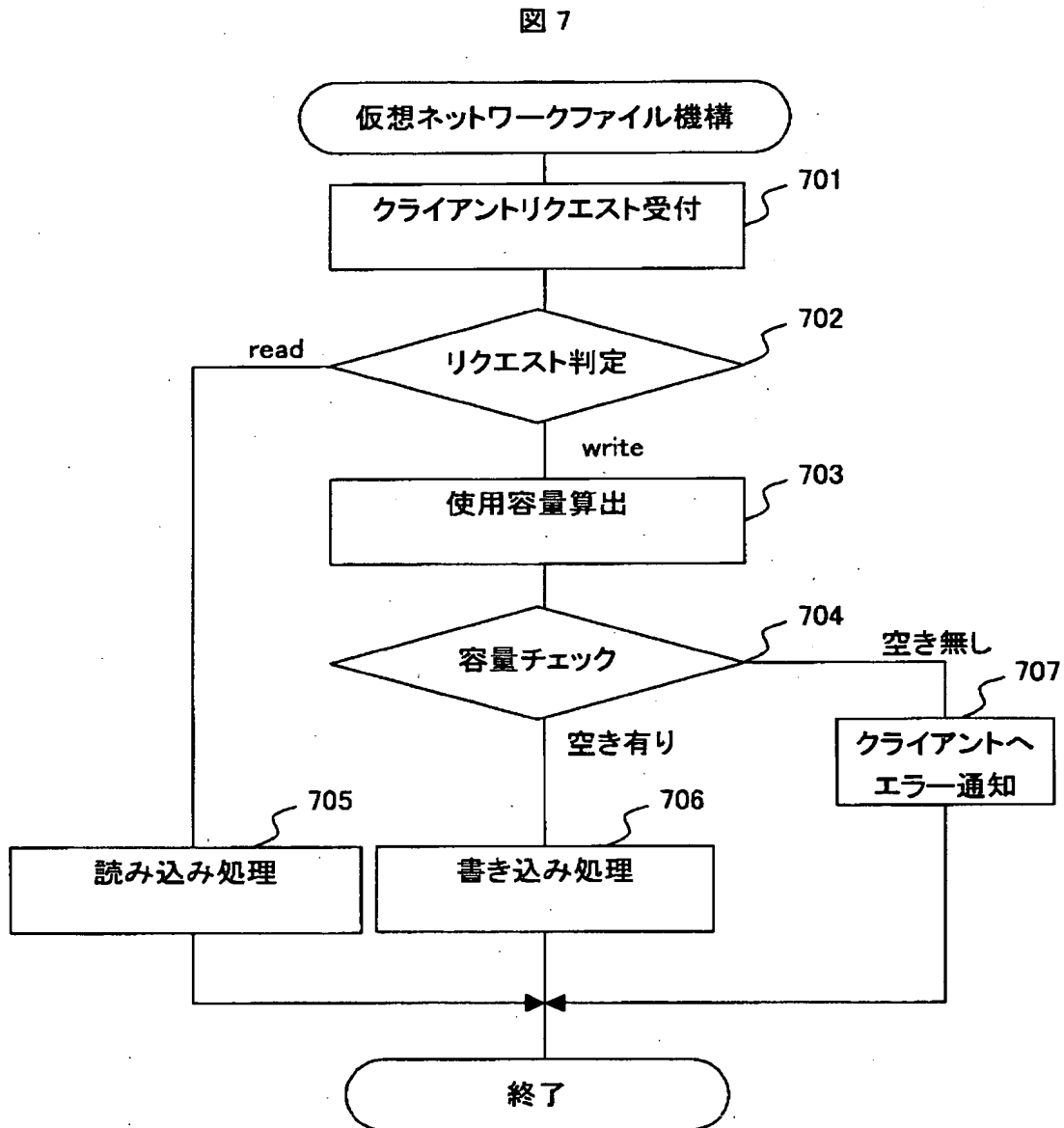


【図 6】

図 6

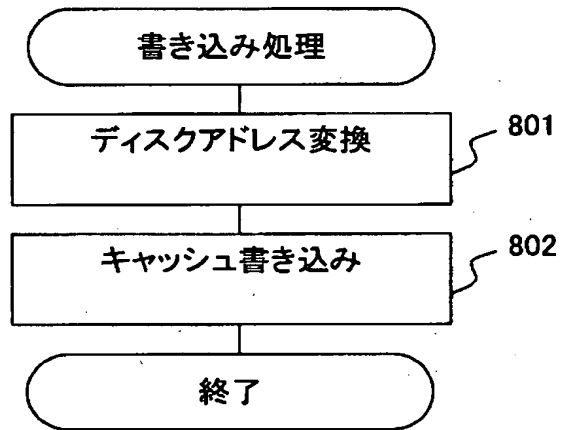


【図 7】

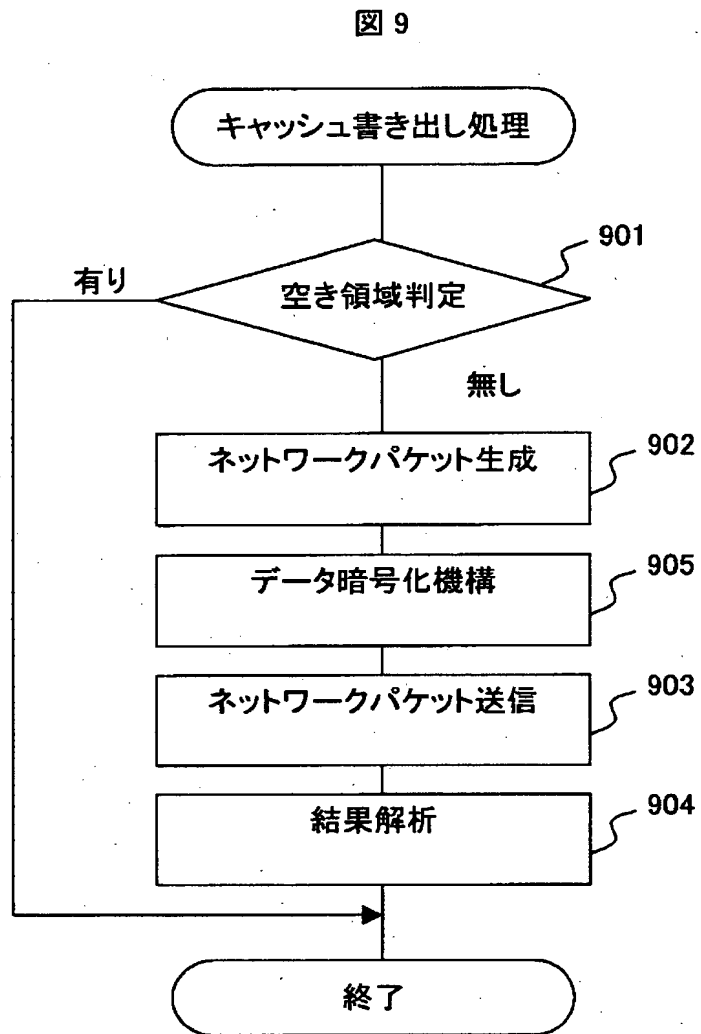


【図 8】

図 8

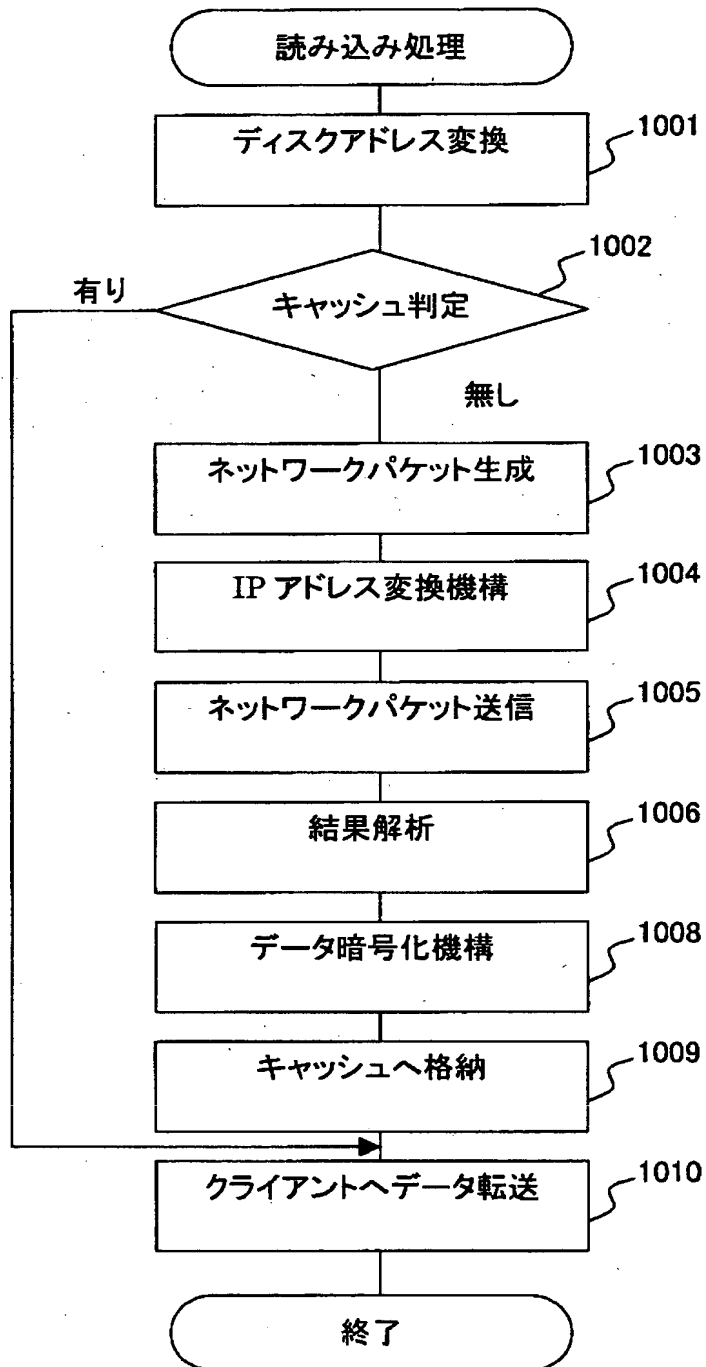


【図9】



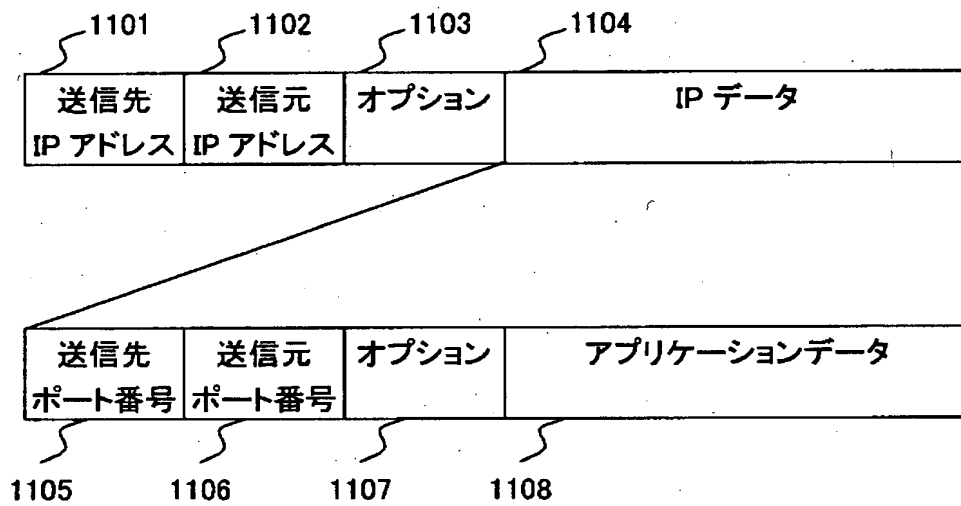
【図 10】

図 10



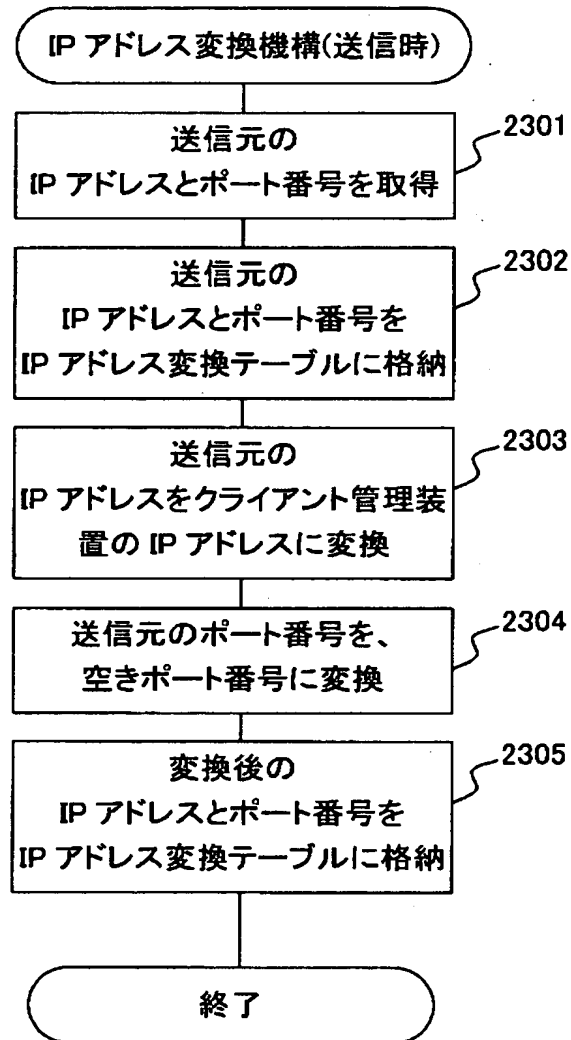
【図 11】

図 11



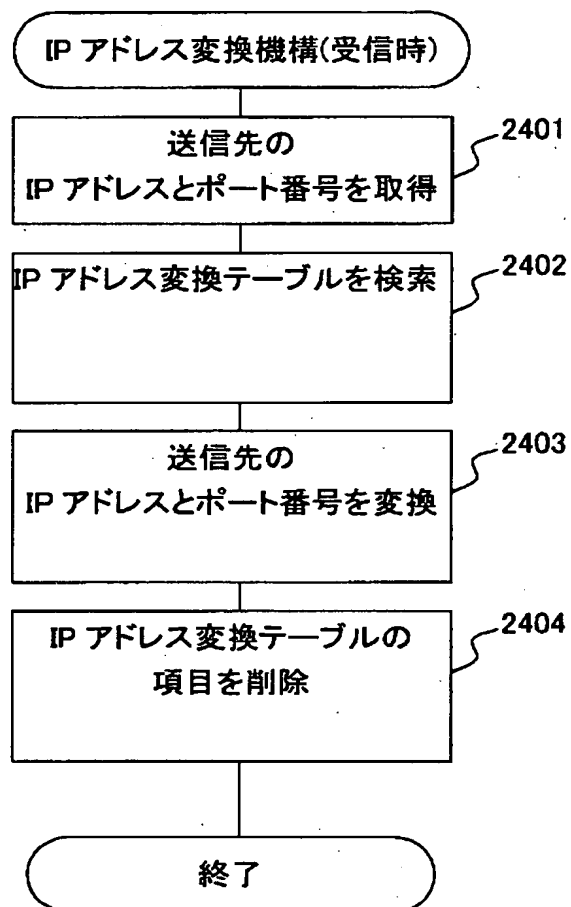
【図 1 2】

図 12



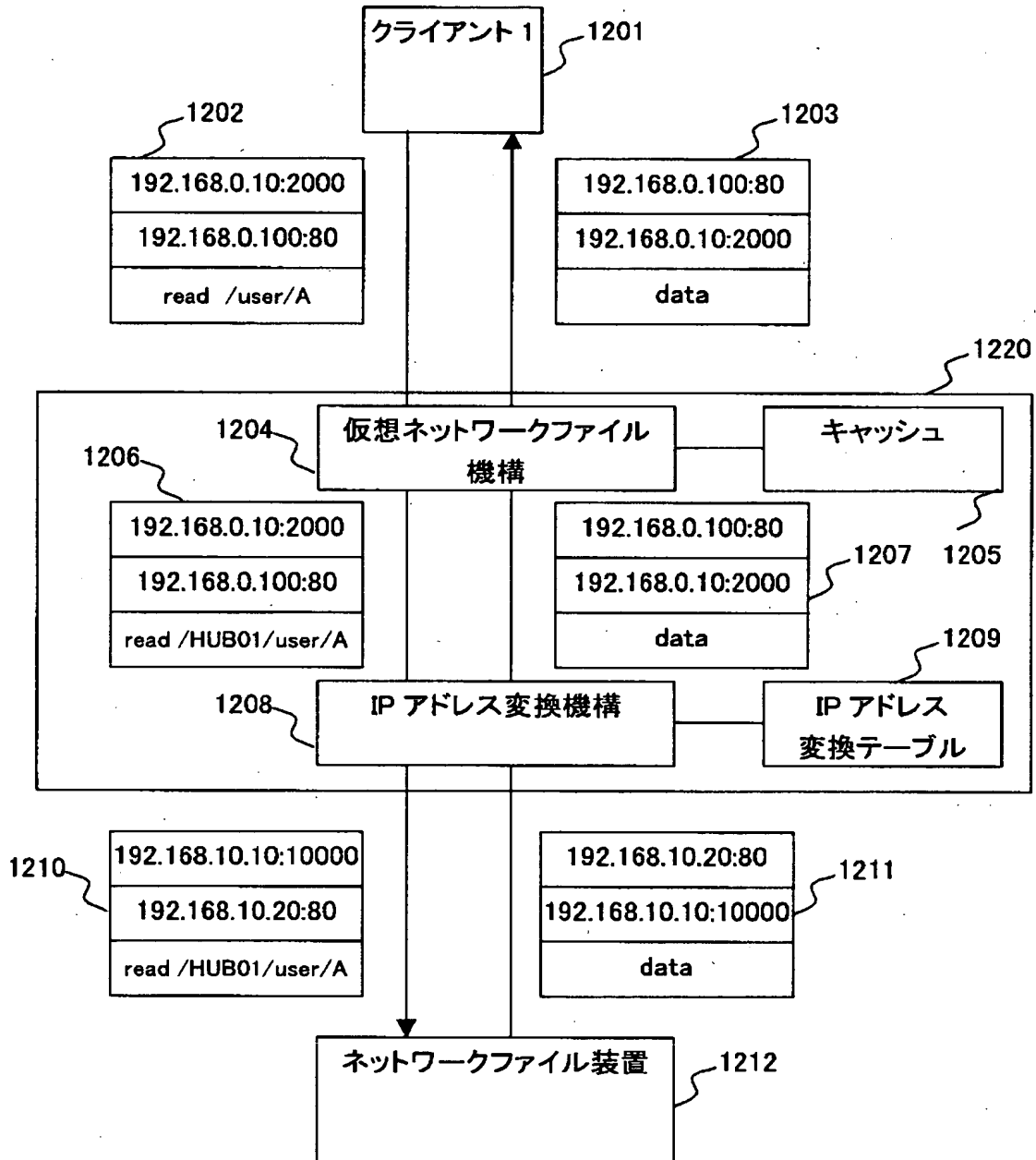
【図 13】

図 13



【図 14】

図 14



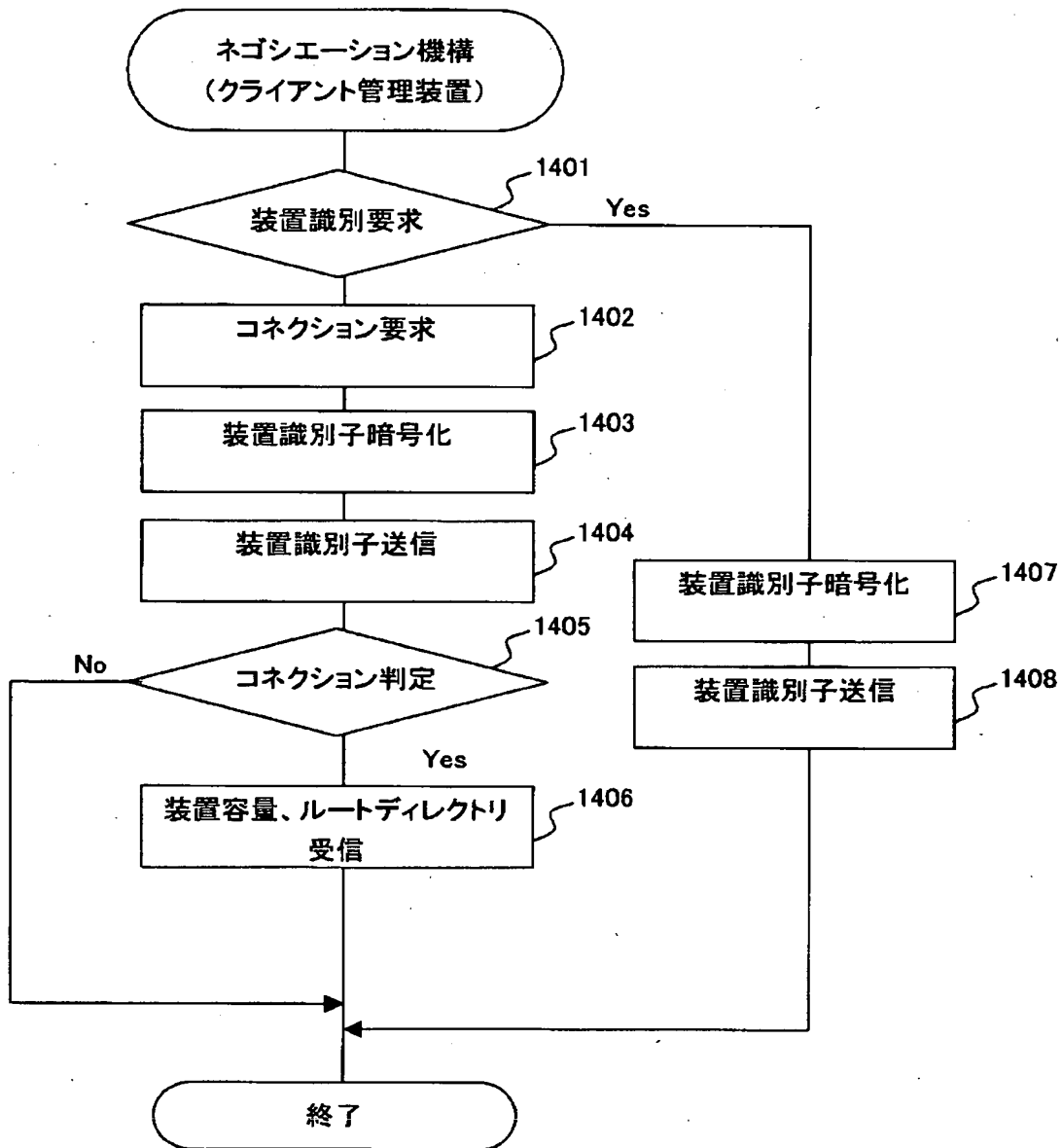
【図 1 5】

図 15

1301 クライアント IP アドレス	1302 クライアント ポート番号	1303 変換後 IP アドレス	1304 変換後 ポート番号
192.168.0.10	2000	192.168.10.10	10000
192.168.0.20	2001	192.168.10.10	10001
...

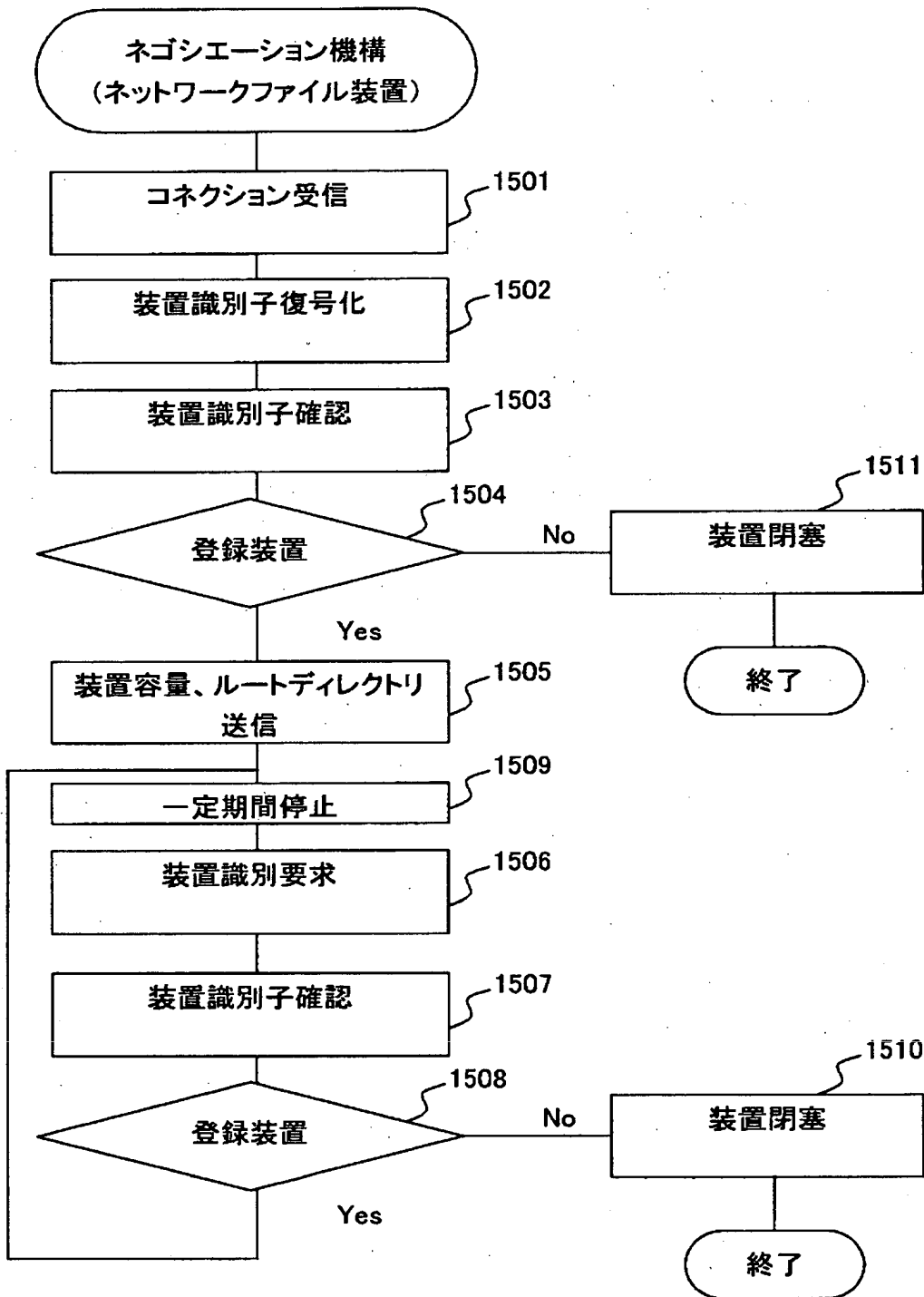
【図 16】

図 16



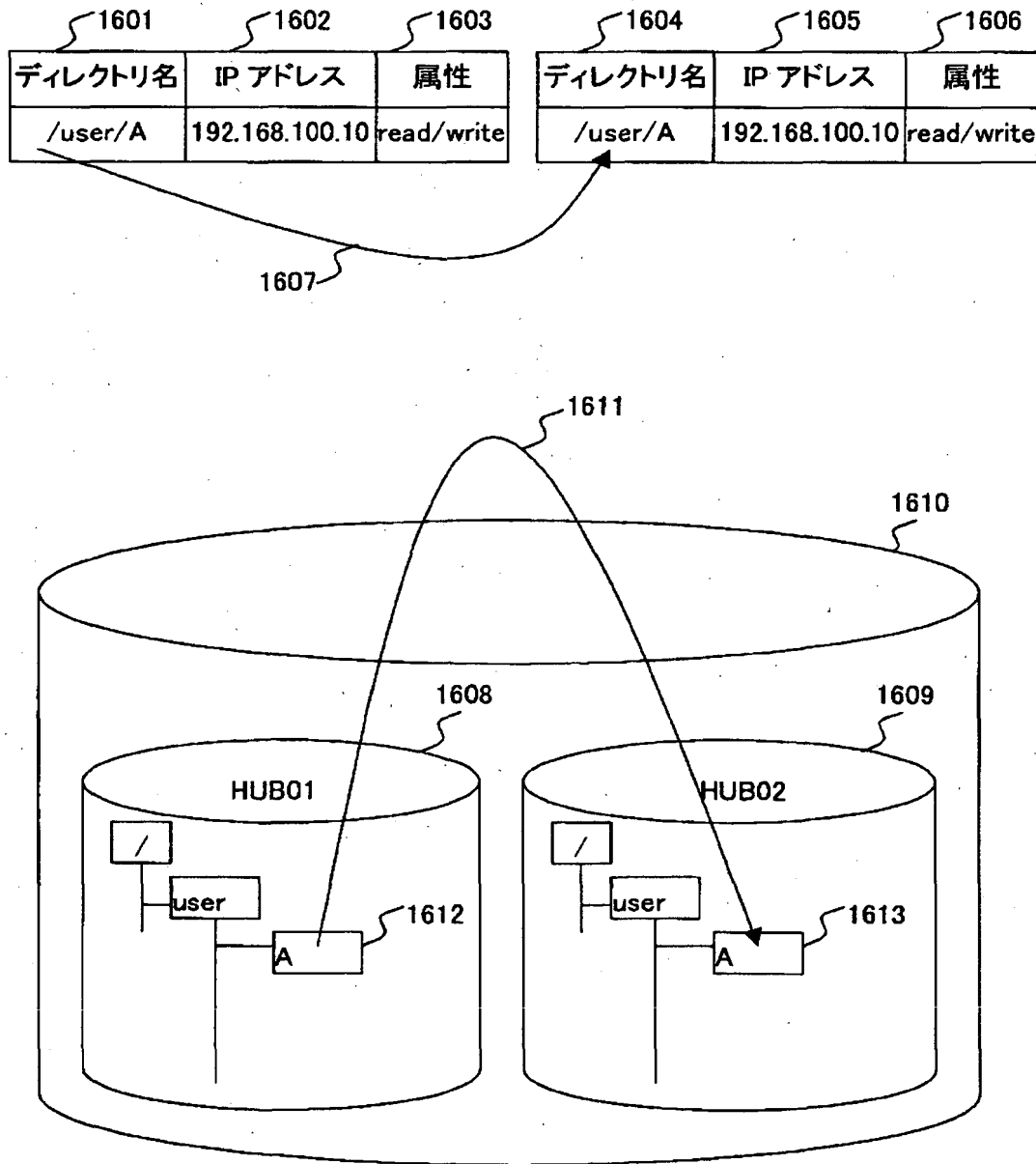
【図 17】

図 17



【図 18】

図 18



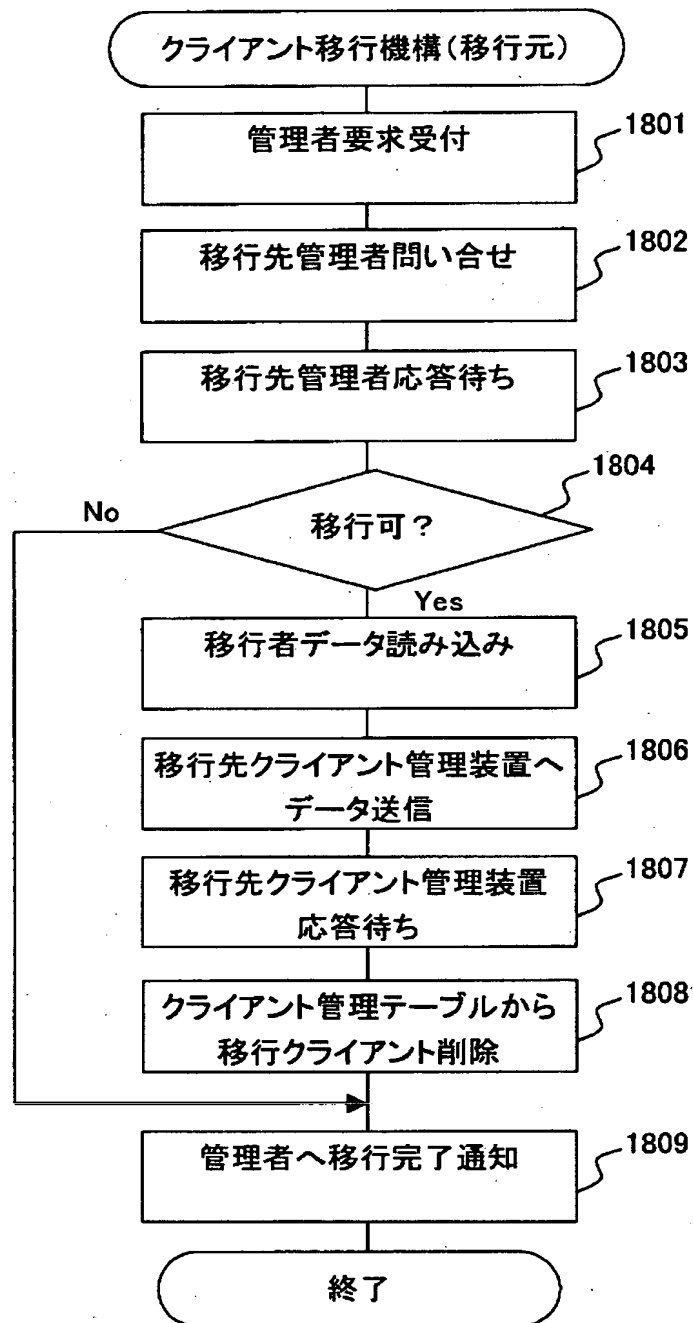
【図 1 9】

図 19

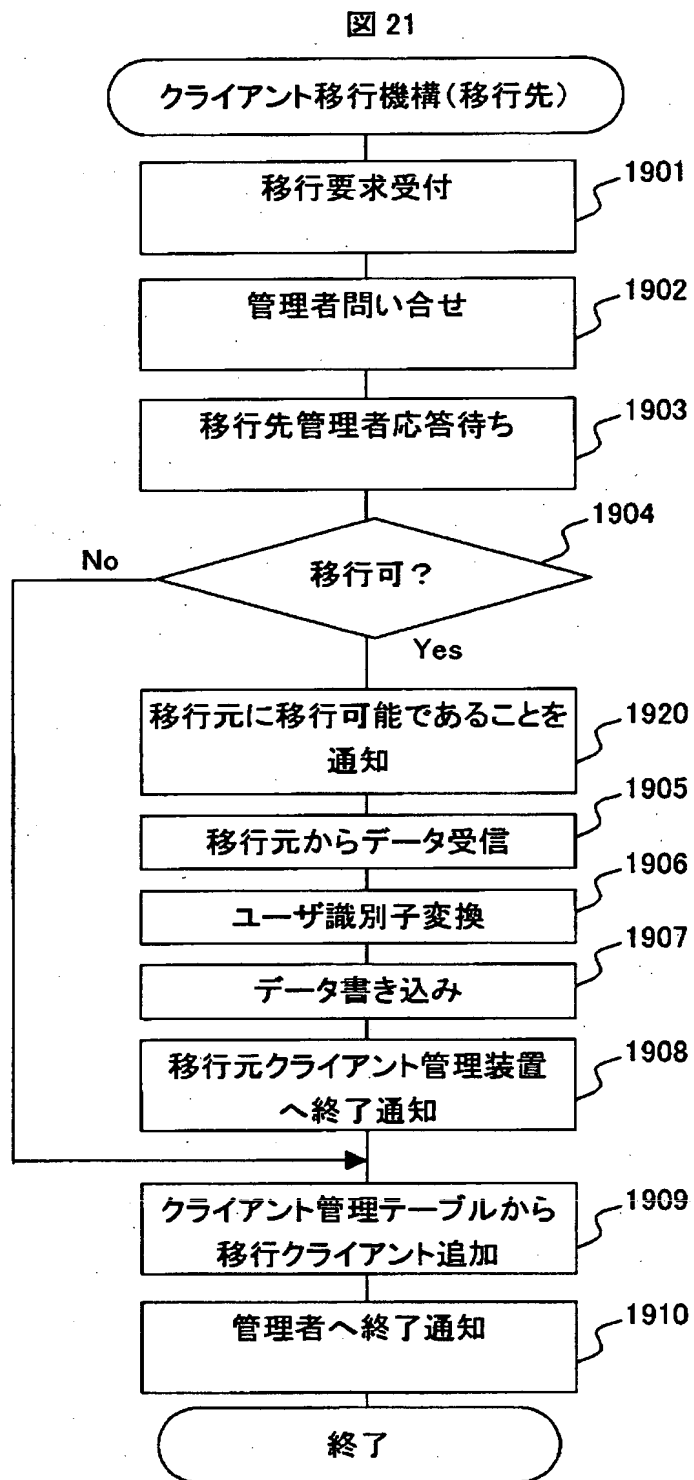
1701 ファイル名	1702 ユーザ識別子	1703 ファイル属性
/user/A/file1	501	rw
/user/A/file2	501	rwx
/user/B/file3	502	r
/user/C/file4	503	rw
/user/C/file5	503	rw

【図 20】

図 20

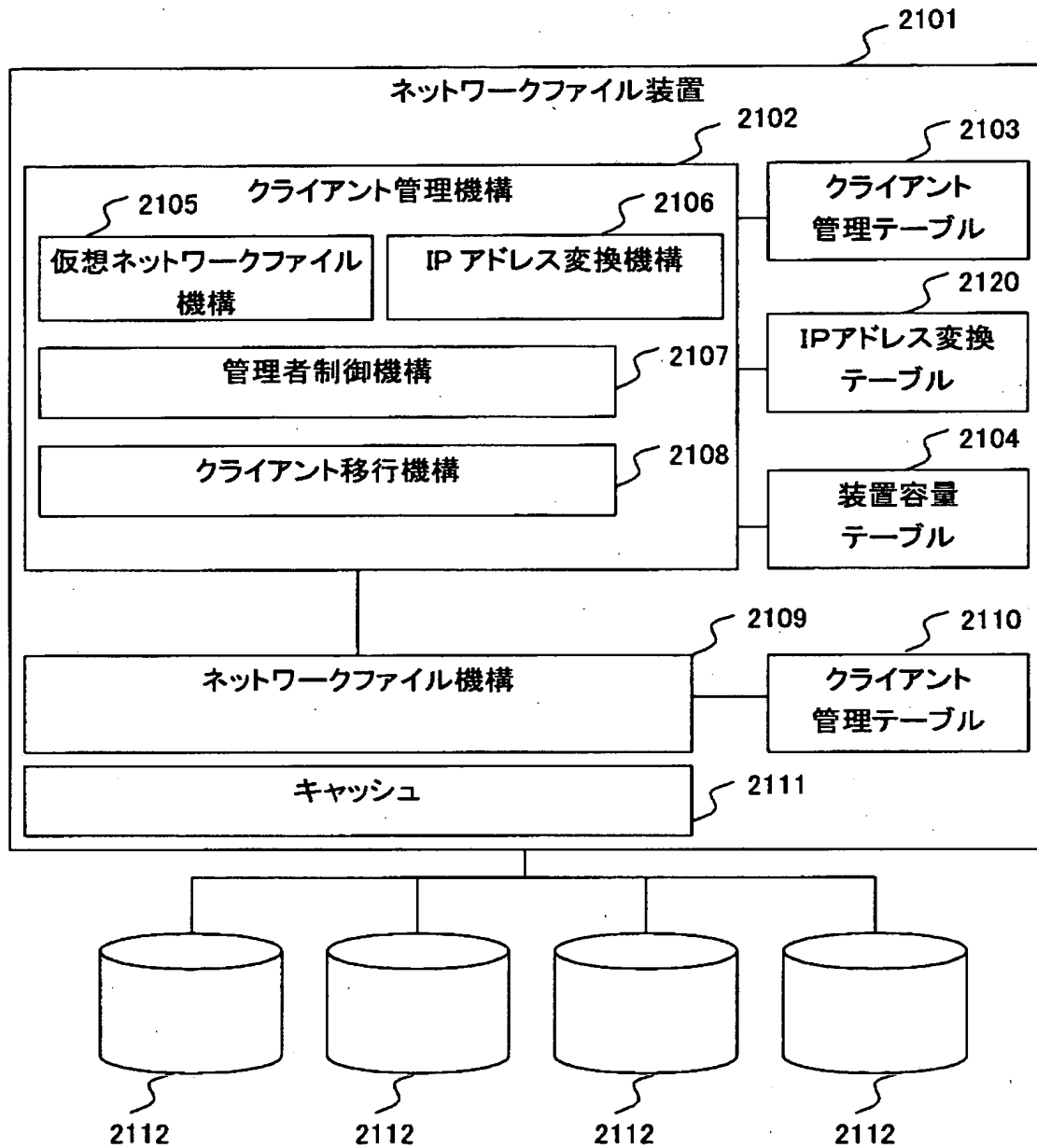


【図 21】



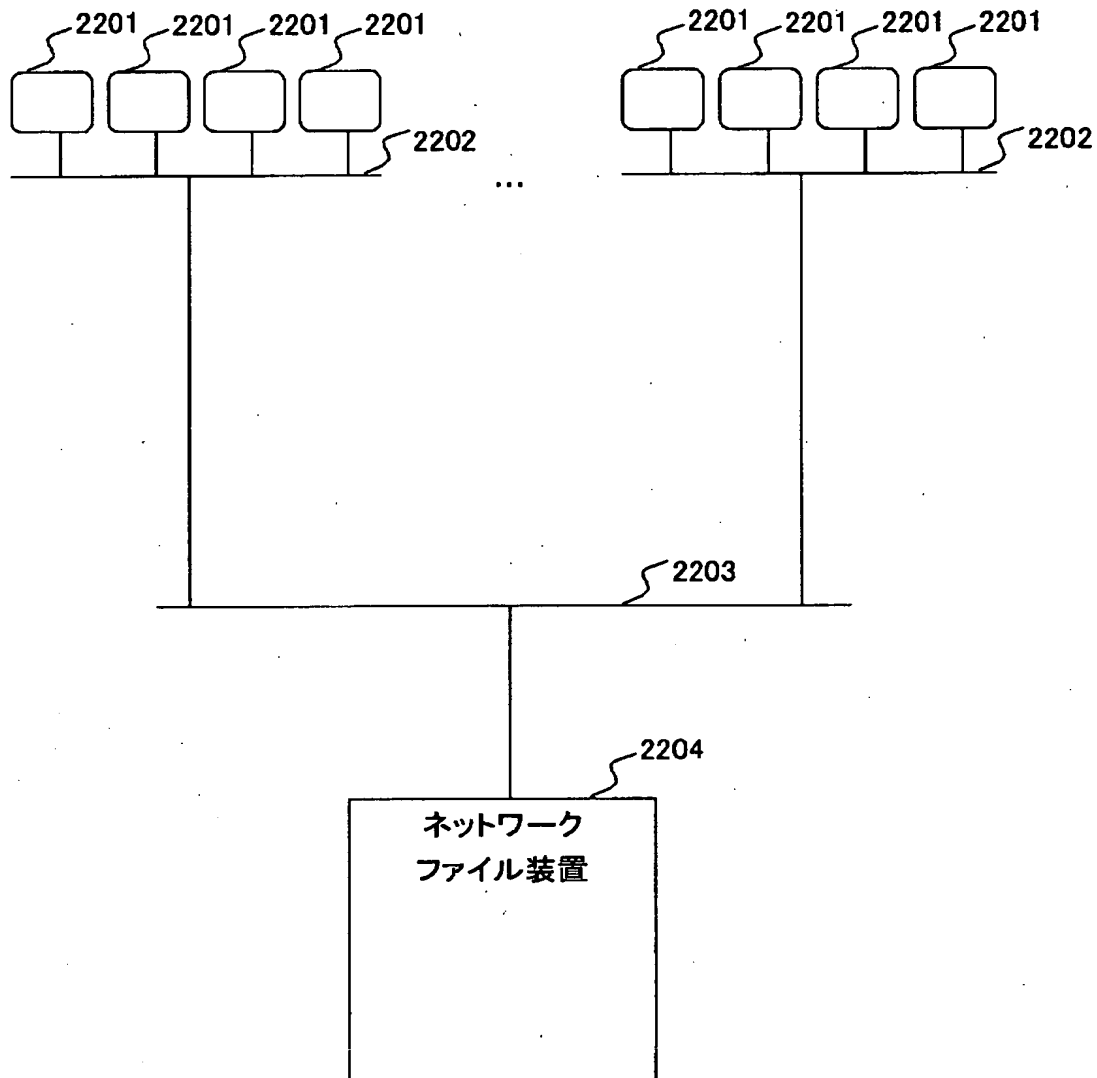
【図 2 2】

図 22



【図 23】

図 23



【書類名】 要約書

【要約】

【課題】 大規模なネットワークファイル装置のクライアント管理を容易にする

【解決手段】 ネットワークファイル装置とクライアントの間にクライアントを管理する装置を設け、管理を階層化する。

【効果】 大規模なクライアント環境でも、階層化することで各管理者は少ないクライアントの管理で済み、管理が容易になる。

【選択図】 図 1

特 2003-010509

認定・付加情報

特許出願の番号	特願 2003-010509
受付番号	50300075237
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 1月21日

<認定情報・付加情報>

【提出日】	平成15年 1月20日
-------	-------------

次頁無

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所